Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

ON THE NUMERICAL FACTORS OF THE ARITHMETIC FORMS $\alpha^n \pm \beta^n$.*

BY R. D. CARMICHAEL.

Continued from page 48.

We shall now show that if $F_{\nu p^a}$ is divisible by p, where ν is prime to p, then $F_\nu{}^2$ is divisible by p. If $\nu = 1$ the result is already contained in the remark following Lemma II. From equation (10) we have

$$F_{\nu p^a}(\alpha, \beta) \cdot F_\nu(\alpha^{p^{a-1}}, \beta^{p^{a-1}}) = F_\nu(\alpha^{p^a}, \beta^{p^a}).$$

If $\nu > 1$ Lemma I is applicable, and we have

$$F_{\nu p^a}(\alpha, \beta) \cdot F_\nu(\alpha, \beta) \equiv F_\nu(\alpha, \beta) \bmod p.$$

Hence if

$$F_\nu(\alpha, \beta) \not\equiv 0 \bmod p,$$

then

$$F_{\nu p^a}(\alpha, \beta) \equiv 1 \bmod p,$$

contrary to the hypothesis that

$$F_{\nu p^a}(\alpha, \beta) \equiv 0 \bmod p.$$

From this argument we see also that when $\nu > 1$ and $F_{\nu p^a}$ is not divisible by p, then

$$F_{\nu p^a} \equiv 1 \bmod p.$$

If $\nu = 1$, we have

$$F_{p^a} \equiv (\alpha - \beta)^{(p-1)} \bmod p$$

if p is odd, as may readily be shown by means of the remark following lemma II. Evidently,

$$F_{2^a} \equiv 1 \bmod 2$$

when

$$F_{2^a} \not\equiv 0 \bmod 2.$$

Combining the several results obtained above we have the following fundamental theorem:

THEOREM XIV. *Let ν be any positive integer and let p be any prime not dividing ν; then*

(1) *If $F_{\nu p^a} \equiv 0 \bmod p$, then $F_\nu{}^2 \equiv 0 \bmod p$.*

(2) *If $F_\nu{}^2 \equiv 0 \bmod p$, then each of the numbers $F_{\nu p}, F_{\nu p^2}, F_{\nu p^3}, \cdots$ is divisible by p, and none of them is divisible by p^2 except when $\nu = 1$ in which*

case F_p may be divisible by a power of p[*] *and when $\nu = 3$, $p = 2$ in which case F_6 may be divisible by 2^2. Moreover, $F_{k^2} \not\equiv 0 \bmod p$ unless k is of the form νp^a.*

(3) *If $F_{\nu p^a} \not\equiv 0 \bmod p$, $a > 0$, then $F_{\nu p^a} \equiv 1 \bmod p$ when $\nu > 1$ or when $\nu = 1$ and $p = 2$; if $\nu = 1$ and p is odd we have*

$$F_{p^a} \equiv (\alpha - \beta)^{(p-1)} \equiv \pm 1 \bmod p.$$

Let m and n be any two positive integers different from each other and from unity. We enquire what is the greatest common divisor of $F_m(\alpha, \beta)$ and $F_n(\alpha, \beta)$. If p is a prime divisor of each of these numbers it follows from the preceding theorem that there exists a number ν prime to p such that

$$F_{\nu^2} \equiv 0 \bmod p, \qquad m = \nu p^a, \qquad n = \nu p^b;$$

whence we conclude further that F_m and F_n contain p but not p^2 as a common factor. If a second prime number q is a factor of both numbers we have $m = \mu q^c$ and $n = \mu q^d$ where μ is prime to q; whence

$$\nu p^a = \mu q^c \quad \text{and} \quad \nu p^b = \mu q^d; \quad \text{or} \quad \frac{\mu}{\nu} = \frac{p^a}{q^c} = \frac{p^b}{q^d}.$$

Therefore $a = b$ and $c = d$; that is, $m = n$, contrary to the hypothesis. From these considerations we have readily the following theorem:

THEOREM XV. *If m and n are positive integers different from each other and from unity, then the greatest common divisor of $F_m(\alpha, \beta)$ and $F_n(\alpha, \beta)$ is unity or a prime p: a necessary and sufficient condition that it is p is that there exists a ν such that*

$$F_{\nu^2} \equiv 0 \bmod p, \quad m = \nu p^a \quad \text{and} \quad n = \nu p^b.$$

If p is any prime number which does not divide $\alpha\beta$ then p is a factor of one of the numbers D_{p-1}, D_p, D_{p+1}, as we saw in the preceding section. From Theorem IV it follows then that p is a factor of one number at least of the set $F_2, F_3, \cdots, F_{p+1}$. Now if $F_{\nu p^a}$ is divisible by p so is F_{ν^2}, ν being prime to p; moreover, F_{k^2} is not divisible by p if k is less than ν, as we see from Theorem XIV. Hence ν is not greater than $p + 1$. In particular ν does not contain a prime factor greater than p if p is odd. We may apply this result to the problem of finding the greatest common divisor of m and $F_m(\alpha, \beta)$. We see at once that the greatest common odd divisor of these numbers is 1 or p, where p is the greatest odd prime factor of m; and that if this divisor is p and $m = \nu p^a$ where ν is prime to p, then ν is not greater than $p + 1$. There are two cases in which m and F_m may have the factor

---

[*] But if α and β are integers and p is odd it is easy to show that F_p is not divisible by p^2.

2 in common. If F_2 is divisible by 2 and m is a power of 2, then m and F_m have the greatest common divisor 2. If F_3 is divisible by 2 and m is of the form 3.2^t, then m and F_m have the factor 2 in common but not the factor 2^2. If $t = 1$ or 2 and F_{2^t} is divisible by 3 they contain also the common factor 3. These results may be put into the following theorem:

THEOREM XVI. *The greatest common odd divisor of m and $F_m(\alpha, \beta)$ is* 1 *or p, where p is the greatest odd prime factor of m; if this divisor is p and $m = \nu p^a$, where ν is prime to p, then ν is not greater than $p + 1$. These numbers contain in addition the common factor* 2 *(but not 2^2) in two cases: (a) when F_2 is divisible by* 2 *and m is a power of* 2; *(b) when F_3 is divisible by* 2 *and m is of the form 3.2^t.*

Now, when m is greater than 1,

$$D_m = \Pi F_d(\alpha, \beta),$$

where d runs over the divisors of m except unity. The number F_{mp}, where p is prime, has no factor in common with any F_d other than a common factor of d and mp. Hence every common prime factor of D_m and F_{mp} is likewise a factor of mp. Suppose that D_m and F_{mp} have a common prime factor q different from p. Then some F_d contains the factor q; and hence q is a divisor of some $F_\nu{}^2$ where ν is prime to q, as we see from Theorem XIV; and therefore (Theorem XIV) q is not a divisor of F_{mp}. Hence D_m and F_{mp} contain no common prime factor other than p. Again applying Theorem XIV we see that the greatest common divisor of D_m and F_{mp} is 1 or p. Hence we have the following theorem:

THEOREM XVII. *If p is a prime number then the greatest common divisor of D_m and F_{mp} is* 1 *or p.*

COROLLARY. *The greatest common divisor of D_m and D_{mp}/D_m is* 1 *or p.*

For, we have

$$\frac{D_{mp}}{D_m} = \Pi F_{kp},$$

where kp runs over those divisors of mp which are not at the same time divisors of m. Now the greatest common divisor of F_{kp} and D_m is a divisor of D_k, since k is obviously the greatest common divisor of m and kp. But the greatest common divisor of D_k and F_{kp} is 1 or p. Also, not more than one of the numbers F_{kp} contains the factor p, as one sees from Theorem XIV, since all the subscripts kp contain p to the same power. Hence the corollary.

We shall now consider a different kind of property of $F_n(\alpha, \beta)$. Denote by P_n the greatest factor of F_n which is prime to n; and write

$$F_n = \lambda P_n.$$

From Theorems XIV and XVI we see that $|\lambda|$ is unity or is the greatest prime factor of n except possibly when n is of the form 3.2^t in which case it is a power of 2 or such a power multiplied by 3 or when $n = p$, a prime number, in which case $|\lambda|$ may be a power of p. The question arises as to the possibility that P_n shall be equal to 1; and to this we turn attention.

There are two cases in which the results are of essentially different character: (1) when $|\alpha| = |\beta|$, in which case it is obvious that α and β are complex quantities; (2) when $|\alpha| \neq |\beta|$, in which case α and β are real. In the former case P_n may be equal to unity for various values of n, as the following examples show:

(1) When

$$\alpha + \beta = 1, \qquad \alpha\beta = 2,$$

we have

$$D_{n+2} = D_{n+1} - 2D_n;$$

and therefore we may readily determine the following values:

$$n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18,$$

$$D_n = 1, 1, -1, -3, -1, 5, 7, -3, -17, -11, 23, 45, -1, -91, -89, 93, 271, 85,$$

$$P_n = 1, 1, 1, 3, 1, 5, 1, 1, 17, 11, 23, 1, 1, 13, 89, 31, 271, 1.$$

Here $P_n = 1$ for $n = 1, 2, 3, 5, 7, 8, 12, 13, 18$.

(2) When $\alpha + \beta = 5$, $\alpha\beta = 7$, we have

$$F_{10} = \frac{\alpha^5 + \beta^5}{\alpha + \beta} = -5.$$

Hence in this case $P_{10} = 1$.

(3) If $\alpha + \beta = 2$, $\alpha\beta = 7$, then $F_8 = \alpha^4 + \beta^4 = 2$. Hence $P_8 = 1$.

(4) If $\alpha + \beta = 3$, $\alpha\beta = 4$, then $P_4 = 1$, $P_6 = 1$.

These examples show that for appropriate values of α and β $P_n(\alpha, \beta)$ may be unity for various values of n; in particular for all values less than 14 except possibly 9 and 11. It is to be noted, however, that in all these examples $|\alpha| = |\beta|$. If α and β are real, and hence $|\alpha| \neq |\beta|$, we have a different state of affairs as will now be proved. The treatment will fall into two parts, according as α and β are of the same or of different sign.

Let us suppose first that the real quantities α and β are of the same sign. Without loss of generality we may take them to be positive; and this we do. Further, since

$$F_n(\alpha, \beta) = F_n(\beta, \alpha),$$

there is no loss of generality in assuming, as we shall do, that α is greater than β. Now

$$F_2(\alpha, \beta) = \alpha + \beta$$

and this number is to a large extent arbitrary; hence we shall suppose that n is greater than 2. Moreover, there is an infinite number of cases in which $P_6 = 1$, as we see by putting

$$\alpha + \beta = 3 + 2^k, \qquad \alpha\beta = 3 + 2^{k+1},$$

whence

$$F_6 = \alpha^2 - \alpha\beta + \beta^2 = (\alpha + \beta)^2 - 3\alpha\beta = 2^{2k}.$$

Therefore we leave out of consideration entirely the case when $n = 6$.

From equation (9) we have

$$(20) \qquad F_n(\alpha, \beta) = \lambda P_n(\alpha, \beta) = \frac{D_n \cdot \Pi D_{n/p_ip_j} \cdots}{\Pi D_{n/p_i} \cdot \Pi D_{n/p_ip_jp_k} \cdots},$$

where the products denoted by Π extend over the combinations 2, 4, 6, $\cdots$ at a time of p_1, p_2, $\cdots$ in the numerator and over the combinations 1, 3, 5, $\cdots$ at a time in the denominator, p_1, p_2, $\cdots$ being the different prime factors of n.

Now we have

$$D_k = \frac{\alpha^k - \beta^k}{\alpha - \beta} = \alpha^{k-1} + \alpha^{k-2}\beta + \cdots + \beta^{k-1} > \alpha^{k-1}.$$

Applying this inequality to the numerator of the last member of (20) we have

$$D_n \cdot \Pi D_{n/p_ip_j} \cdots > \alpha^\sigma,$$

where

$$\sigma = (n - 1) + \Sigma\left(\frac{n}{p_ip_j} - 1\right) + \Sigma\left(\frac{n}{p_ip_jp_kp_l} - 1\right) + \cdots$$

$$= n - 2^{m-1} + \Sigma\frac{n}{p_ip_j} + \Sigma\frac{n}{p_ip_jp_kp_l} + \cdots,$$

where m is the number of different prime factors of n.

Now

$$D_k = \frac{\alpha^k - \beta^k}{\alpha - \beta} < \frac{\alpha^k}{\alpha - \beta} < \alpha^k,$$

since $(\alpha - \beta)^2$ is an integer and $\alpha - \beta$ is positive. Applying this inequality to the denominator of the last member of (20) we have

$$\Pi D_{n/p_i} \cdot \Pi D_{n/p_ip_jp_k} \cdots < \alpha^\tau,$$

where

$$\tau = \Sigma\frac{n}{p_i} + \Sigma\frac{n}{p_ip_jp_k} + \cdots.$$

By division we see that the last member of (20) is greater than $\alpha^{\sigma-\tau}$. Now

$$\sigma - \tau = -2^{m-1} + n - \Sigma\frac{n}{p_i} + \Sigma\frac{n}{p_ip_j} - \Sigma\frac{n}{p_ip_jp_k} + \cdots$$
$$= \varphi(n) - 2^{m-1},$$

where $\varphi(n)$ is Euler's φ-function of n, since

$$\varphi(n) = n - \Sigma\frac{n}{p_i} + \Sigma\frac{n}{p_ip_j} - \cdots.$$

Therefore

(22) $$F_n(\alpha, \beta) = \lambda P_n(\alpha, \beta) > \alpha^{\phi(n)-2^{m-1}}.$$

If we apply the inequality $D_k < \alpha^k$ to the numerator of (20) and the inequality $D_k > \alpha^{k-1}$ to its denominator we find that

(23) $$F_n(\alpha, \beta) = \lambda P_n(\alpha, \beta) < \alpha^{\phi(n)+2^{m-1}}.$$

Now

$$(\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta.$$

Since $\alpha - \beta$ is real and different from zero we have $(\alpha + \beta)^2 > 4\alpha\beta$. But $\alpha\beta$ is a positive integer, according to our present hypothesis; and hence

$$\alpha + \beta \geqq 3.$$

Also,

$$\alpha - \beta \geqq 1.$$

Hence $\alpha \geqq 2$. This fact is of use in connection with relations (22) and (23).

It is obvious that

$$\varphi(n) \geqq 2^{m-1}.$$

Hence from relation (22) we see that if $P_n = 1$ then $\lambda > 1$. Hence if n is neither an odd prime nor of the form 3.2^t, $t > 1$, we must have λ equal to the greatest prime factor of n, since, as we have seen before, this is now the only possible value of λ different from unity.

Let us consider first the case when n is of the form $n = 3.2^t$. Here we have from (22),

$$\lambda P_n(\alpha, \beta) > \alpha^{2^{t}-2} \geqq 2^{2^{t}-2},$$

where λ has one of the values 2, 3, 6 (Theorems XIV and XVI). Hence if $t > 2$ we have $P_n > 1$. Hence we have to examine further only the case when $t = 2$. To show that $P_{12} > 1$ it is sufficient to show that $F_{12} > 6$. Since $(\alpha + \beta)^2 - 4\alpha\beta > 0$ we have $\alpha^2 + \beta^2 > 2\alpha\beta$; and therefore

$$F_{12} \equiv \alpha^4 - \alpha^2\beta^2 + \beta^4 = (\alpha^2 + \beta^2)^2 - 3\alpha^2\beta^2 > \alpha^2\beta^2.$$

Hence $F_{12} > 6$ unless $\alpha\beta \leqq 2$. Considering this case we see that

$$\alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta \geqq 9 - 4 = 5,$$

since

$$\alpha + \beta \geqq 3.$$

Hence

$$F_{12} \geqq 5^2 - 12 > 6.$$

Hence $P_{12} > 1$ for every positive α and β.

We consider next the case when λ is equal to the greatest prime factor of n. Call this factor p and write $n = \nu p^a$, where ν is prime to p. Suppose first that ν is not unity (whence $p > 2$). Applying relation (23) we have

$$F_\nu(\alpha, \beta) < \alpha^{\phi(\nu)+2^{m-2}}. \tag{23'}$$

Now

$$F_\nu(\alpha, \beta) \equiv 0 \bmod p,$$

as we see from Theorem XIV, since in the present case p is a factor of $F_n(\alpha, \beta)$. But $F_\nu(\alpha, \beta)$ is different from zero; and hence it is equal to or greater than p. Therefore

$$P_n(\alpha, \beta) = \frac{F_n(\alpha, \beta)}{p} \geqq \frac{F_n(\alpha, \beta)}{F_\nu(\alpha, \beta)} > \alpha^{\phi(n)-\phi(\nu)-3\cdot 2^{m-2}};$$

the last term in this relation is obtained by aid of (22) and (23′). Hence $P_n > 1$ except when $\varphi(n) - \varphi(\nu) - 3.2^{m-2}$ is negative. Now

$$\varphi(n) = p^{a-1}(p-1)\varphi(\nu);$$

and therefore the exponent above may be written in the form

$$\varphi(\nu)[p^{a-1}(p-1) - 1] - 3.2^{m-2}.$$

Since

$$\varphi(\nu) \geqq 2^{m-2}$$

the expression above can be negative only when $p^{a-1}(p-1) - 1 < 3$. Since $p \neq 2$, this condition can be satisfied only when $p^a = 3$. Then n is of the form 3.2^t, a case which we have already treated.

In case $\nu = 1$ we have from (22)

$$pP_{p^a} > 2^{p^{a-1}(p-1)-1} \geqq 2^{p-2}.$$

If we now assume that $P = 1$ it follows from the last term of these inequalities that $p = 2$ or 3, since $2^{p-2} > p$ when $p \geqq 5$. Then from the middle term we see that a must be unity. Therefore, since we are leaving out of consideration the case when $n = 2$, we have to examine further only the case when

$$n = p^a = 3.$$

Now

$$F_3(\alpha, \beta) = \alpha^2 + \alpha\beta + \beta^2 = (\alpha + \beta)^2 - \alpha\beta > 3\alpha\beta,$$

since $(\alpha + \beta)^2 > 4\alpha\beta$. Hence $F_3 > 3$, so that in this case $P_3 > 1$.

There yet remains the case when n is equal to an odd prime p and $\lambda = p^s$, where s is an integer greater than unity. We have seen (footnote to Theorem XIV) that in this case α and β are not integers. If $P_p = 1$ we have $F_p = p^s$. Now from Lemma II in § 3 and the fact that $D_p = F_p$ we have

$$F_p \equiv (\alpha - \beta)^{p-1} \bmod p.$$

And hence the condition $F_p = p^s$ cannot be satisfied unless p is a factor of $(\alpha - \beta)^2$. As an example to show that this possibility can actually arise we have

$$\alpha + \beta = 3^k + 1, \qquad \alpha\beta = \tfrac{1}{4}\{(3^k + 1)^2 - 3(3^k - 1)^2\},$$

$$F_3(\alpha, \beta) = (\alpha + \beta)^2 - \alpha\beta = 3^{k+1},$$

where k is any positive integer.

Thus we are led to the following preliminary result:

If α and β are real and of the same sign and $n \neq 1, 2, 6$, then $F_n(\alpha, \beta)$ contains a factor (other than unity) which is prime to n except when α and β are suitably chosen irrational numbers and, at the same time, n is equal to an odd prime factor of $(\alpha - \beta)^2$.

COROLLARY.* *If a and b are relatively prime positive integers, $a > b$, and $n > 2$, then $F_n(a, b)$ contains a factor (other than unity) which is prime to n except when $n = 6$, $a = 2$, $b = 1$.* (Compare the more general result in Theorem XIX.)

To complete the proof of the corollary it is sufficient to show that $a = 2$ and $b = 1$ are the only positive integer values of a and b, $a > b$, for which

$$F_6 \equiv a^2 - ab + b^2 = 2^k \cdot 3^\rho,$$

k and ρ being integers; and this is easily done.

Let us turn now to the case when α and β are real but of different sign. As before, we exclude from consideration the cases $n = 1, 2, 6$. Since

$$P_n(\beta, \alpha) = P_n(\alpha, \beta) = P_n(-\alpha, -\beta)$$

we may without loss of generality assume that α is positive and greater than $|\beta|$; and this we do. Now

$$(\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta \overset{=}{>} 5.$$

Hence

$$\alpha - \beta \overset{=}{>} \sqrt{5} > 2.$$

Also,

$$\alpha + \beta \overset{=}{>} 1.$$

Hence $\alpha > 3/2$. These inequalities will be useful in the sequel.

---

[*] The theorem of the corollary is due to Birkhoff and Vandiver, l. c., pp. 177–179. Compare their method of treatment with that in the text.

We have

$$D_{2k} = \frac{\alpha^{2k} - \beta^{2k}}{\alpha^2 - \beta^2}(\alpha + \beta) = (\alpha + \beta)(\alpha^{2k-2} + \alpha^{2k-4}\beta^2 + \cdots + \beta^{2k-2}) > \alpha^{2k-2};$$

$$D_{2k} < \frac{\alpha^{2k}}{\alpha - \beta} < \frac{\alpha^{2k}}{2};$$

$$D_{2k+1} = \frac{\alpha^{2k+1} - \beta^{2k+1}}{\alpha - \beta} > \frac{\alpha^{2k+1}}{2\alpha} = \frac{\alpha^{2k}}{2} > \alpha^{2k-2};$$

$$D_{2k+1} < \frac{2\alpha^{2k+1}}{\alpha} = 2\alpha^{2k} < \alpha^{2k+2}.$$

1. Now suppose that n is a multiple of 4. Applying the inequality $D_{2k} < \frac{1}{2}\alpha^{2k}$ to the denominator of (20) we have

$$\Pi D_{n/p_i} \cdot \Pi D_{n/p_ip_jp_k} \cdots < 2^{-2^{m-1}}\alpha^{\tau},$$

where

$$\tau = \Sigma\frac{n}{p_i} + \Sigma\frac{n}{p_ip_jp_k} + \cdots,$$

m being as before the number of different prime factors of n. Likewise by means of the inequality $D_{2k} > \alpha^{2k-2}$ we see that

$$D_n \cdot \Pi D_{n/p_ip_j} \cdots > \alpha^{\sigma},$$

where

$$\sigma = -2^m + n + \Sigma\frac{n}{p_ip_j} + \cdots.$$

Hence by division in the last member of (20) and further reduction we have

$$F_n(\alpha, \beta) = \lambda P_n(\alpha, \beta) > 2^{2^{m-1}}\alpha^{\phi(n)-2^m} > \alpha^{\phi(n)} > 2^{\frac{1}{2}\phi(n)}, \tag{24}$$

since $\alpha^2 > 2$.

If n is a power of 2 then λ is 1 or 2 (Theorem XVI); and hence we see from (24) that P_n cannot in this case be unity. Furthermore if $P_n = 1$ n can contain no odd prime factor greater than 3; for when n contains the odd prime factor p the last exponent in (24) is equal to or greater than $p - 1$ and $2^{p-1} > 2p$ unless $p = 3$, and hence greater than λ. It is easy to see in a similar manner that n cannot contain 3^2 or 2^3. Hence the only case left for special consideration is that for which $n = 12$. From (24) it follows that $F_{12} > 4$, and hence if $P_{12} = 1$ we must have $\lambda = 6$, since its only possible values (Theorems XIV and XVI) are 1, 2, 3, 6. This requires that $F_{12} = 6$, which we show to be possible when and only when

$$\alpha + \beta = 1, \qquad \alpha\beta = -1.$$

For, from (24) it follows that $F_{12} > \alpha^4$; hence $\alpha < 2$, whence $|\beta| < 2$. Therefore

$$\alpha + \beta = 1.$$

Now

$$F_{12} = \alpha^4 - \alpha^2\beta^2 + \beta^4 = (\alpha + \beta)^4 - 4\alpha\beta(\alpha + \beta)^2 + \alpha^2\beta^2.$$

Hence

$$F_{12} = 1 - 4\alpha\beta + \alpha^2\beta^2 = 6;$$

and therefore

$$\alpha\beta = -1.$$

2. We take next the case when n is odd. If we apply to the denominator in (20) the inequality $D_{2k+1} < 2\alpha^{2k}$ and to the numerator the inequality $D_{2k+1} > \frac{1}{2}\alpha^{2k}$, we obtain the relation

$$F_n(\alpha, \beta) = \lambda P_n(\alpha, \beta) > 2^{-2^m}\alpha^{\phi(n)} > 2^{\frac{1}{2}\phi(n)-2^m}. \tag{25}$$

Now λ is unity or the greatest odd prime factor of n.* Assuming $P_n \neq 1$ it is easy to see from the above inequalities that n does not contain as many as three different prime factors; that if it contains two prime factors one of these must be 3 and the other 5 or 7, while no one of them is repeated; that if it contains only a single prime factor this prime is not greater than 11 and occurs only to the first power unless it is 3, when it may occur to the second power. Thus we have to examine further only the cases $n = 3$, 3^2, 5, 7, 11, 15, 21. Furthermore we see from (25) that λ cannot be unity except possibly in the case $n = 3$, so that if $P_n = 1$ we have F_n equal to the greatest prime factor of n except possibly when $n = 3$.

Now

$$F_3 = \alpha^2 + \alpha\beta + \beta^2 = (\alpha + \beta)^2 - \alpha\beta \geqq 2.$$

Hence if $P_3 = 1$, $\lambda = 3$ and $F_3 = 3$,—an equation which can be satisfied when and only when

$$\alpha + \beta = 1, \qquad \alpha\beta = -2.$$

Thus we have a single exceptional case when $P_3 = 1$.

If $P_9 = 1$ we must have

$$F_9 = \alpha^6 + \alpha^3\beta^3 + \beta^6 = (\alpha^3 + \beta^3)^2 - \alpha^3\beta^3 = 3,$$

which is clearly impossible. If $P_5 = 1$ we have

$$F_5 = \alpha^4 + \alpha^3\beta + \cdots + \beta^4 = (\alpha + \beta)^4 - 3\alpha\beta(\alpha + \beta)^2 + \alpha^2\beta^2 = 5.$$

Since $\alpha\beta$ is negative it follows readily that this equation can be satisfied when and only when

$$\alpha + \beta = 1, \qquad \alpha\beta = -1.$$

---

* In the text we are tacitly laying aside the case when λ is a power (greater than the first) of the greatest prime factor p of n; for this case, as we have seen, cannot arise unless p is a factor of $(\alpha - \beta)^2$ and $n = p$.

Thus we have here an exceptional case.

If $P_7 = 1$ we have

$$F_7 = \alpha^6 + \alpha^5\beta + \cdots + \beta^6 = (\alpha + \beta)^6 - 5\alpha\beta(\alpha + \beta)^4 + 6\alpha^2\beta^2(\alpha+\beta)^2 - \alpha^3\beta^3 = 7,$$

which is obviously impossible when $\alpha\beta$ is negative. We have

$$F_{11} = D_{11} > \tfrac{1}{2}\alpha^{10} > 2^4 > 11,$$

and therefore $P_{11} \neq 1$. Also,

$$\begin{aligned} F_{15} &= \alpha^8 - \alpha^7\beta + \alpha^5\beta^3 - \alpha^4\beta^4 + \alpha^3\beta^5 - \alpha\beta^7 + \beta^8 \\ &= (\alpha + \beta)^8 - 9\alpha\beta(\alpha + \beta)^6 + 26\alpha^2\beta^2(\alpha + \beta)^4 - 24\alpha^3\beta^3(\alpha + \beta)^2 + \alpha^4\beta^4. \end{aligned}$$

Hence $F_{15} > 5$ when $\alpha\beta$ is negative; and therefore $P_{15} \neq 1$. We have

$$F_{21} = \frac{D_{21}}{D_3 \cdot D_7} > \frac{\frac{1}{2}\alpha^{20}}{2\alpha^2 \cdot 2\alpha^6} = \frac{\alpha^{12}}{2^3} > 2^3 > 7;$$

and hence $P_{21} \neq 1$.

Thus we have completed the investigation of the case when n is odd.

3. Let us consider finally the case in which n is an odd multiple of 2. From the inequalities $D_{2k} > \alpha^{2k-2}$ and $D_{2k+1} > \alpha^{2k-2}$ we see that in general $D_\nu > \alpha^{\nu-3}$; and from the inequalities $D_{2k} < \frac{1}{2}\alpha^{2k}$ and $D_{2k+1} < \alpha^{2k+2}$ we see that $D_\nu < \alpha^{\nu+1}$. Applying the inequalities $D_\nu > \alpha^{\nu-3}$ and $D_\nu < \alpha^{\nu+1}$ to the numerator and the denominator respectively of (20) we obtain without difficulty

$$F_n(\alpha, \beta) = \lambda P_n(\alpha, \beta) > \alpha^{\phi(n)-2^{m+1}}. \tag{26}$$

Now λ is either unity or the greatest prime factor of n. Then, since $\alpha > 3/2$ we see from (26) that if $P_n = 1$ n contains no prime factor greater than 13 and that such prime factor can enter only to the first power except in the case of 3 which may enter to the second power; that if n contains two odd prime factors one of these is 3 and the other is 5 or 7 or 11 while no one of them is repeated; and that n does not contain three different odd prime factors.

Let $n = 2 \cdot 3 \cdot p$ where p is 5, 7 or 11. Then

$$F_{6p} = \frac{D_{6p} \cdot D_p \cdot D_3 \cdot D_2}{D_{3p} \cdot D_{2p} \cdot D_6 \cdot D_1} > \frac{\alpha^{6p-2} \cdot \frac{1}{2}\alpha^{p-1} \cdot \frac{1}{2}\alpha^2 \cdot 1}{2\alpha^{3p-1} \cdot \frac{1}{2}\alpha^{2p} \cdot \frac{1}{2}\alpha^6 \cdot 1} = \tfrac{1}{2}\alpha^{2p-6} > 2^{p-4}.$$

From this inequality it follows that the only possible value for p is 5. For this case we have

$$\begin{aligned} F_{30} &= \alpha^8 + \alpha^7\beta - \alpha^5\beta^3 - \alpha^4\beta^4 - \alpha^3\beta^5 + \alpha\beta^7 + \beta^8 \\ &= (\alpha + \beta)^8 - 7\alpha\beta(\alpha + \beta)^6 + 14\alpha^2\beta^2(\alpha + \beta)^4 - 8\alpha^3\beta^3(\alpha + \beta)^2 + \alpha^4\beta^4 > 5. \end{aligned}$$

Hence $P_{30} \neq 1$.

Suppose next that $n = 2p$, where p is 5, 7, 11 or 13. Then

$$F_{2p} = \frac{D_{2p} \cdot D_1}{D_p \cdot D_2} > \frac{\alpha^{2p-2}}{2\alpha^{p-1} \cdot \frac{1}{2}\alpha^2} = \alpha^{p-3} > \left(\frac{3}{2}\right)^{p-3}.$$

From these relations it follows that $p = 5$ or 7. For $p = 5$ we have

$$F_{10} = \alpha^4 - \alpha^3\beta + \alpha^2\beta^2 - \alpha\beta^3 + \beta^4 = (\alpha + \beta)^4 - 5\alpha\beta(\alpha + \beta)^2 + 5\alpha^2\beta^2 > 5;$$

and hence $P_{10} \neq 1$. For $p = 7$ we have

$$\begin{aligned} F_{14} &= \alpha^6 - \alpha^5\beta + \alpha^4\beta^2 - \alpha^3\beta^3 + \alpha^2\beta^4 - \alpha\beta^5 + \beta^6 \\ &= (\alpha + \beta)^6 - 7\alpha\beta(\alpha + \beta)^4 + 14\alpha^2\beta^2(\alpha + \beta)^2 - 7\alpha^3\beta^3 > 7; \end{aligned}$$

and hence $P_{14} \neq 1$.

There remains yet the case $n = 18$. We have

$$F_{18} = \alpha^6 - \alpha^3\beta^3 + \beta^6 = (\alpha^3 + \beta^3)^2 - 3\alpha^3\beta^3 > 3.$$

Hence $P_{18} \neq 1$.

The various results contained in the immediately preceding discussion may be summarized into the following theorem:

THEOREM XVIII. *If α and β are real and if $n \neq 1, 2, 6$, then $F_n(\alpha, \beta)$ contains a factor (other than unity) which is prime to n in all cases except when: (a) α and β are suitably chosen irrational numbers and n is equal to an odd prime factor of $(\alpha - \beta)^2$;*

(*b*) $n = 3, \quad \alpha + \beta = \pm 1, \quad \alpha\beta = -2;$
(*c*) $n = 5, \quad \alpha + \beta = \pm 1, \quad \alpha\beta = -1;$
(*d*) $n = 12, \quad \alpha + \beta = \pm 1, \quad \alpha\beta = -1.$

The following particular case is of sufficient importance to merit separate statement:

THEOREM XIX. *If a and b are any relatively prime integers and $n > 2$, then $F_n(a, b)$ contains a factor (other than unity) which is prime to n in all cases except when*

(*a*) $n = 3, \quad a + b = \pm 1, \quad ab = -2;$
(*b*) $n = 6, \quad a + b = \pm 3, \quad ab = 2.$

To complete the proof of this theorem it is further necessary (and sufficient) to determine the general solution in relatively prime integers $a + b$ and ab of the equation

$$F_6(a, b) = a^2 - ab + b^2 = (a + b)^2 - 3ab = 2^k \cdot 3^\rho,$$

where k and ρ are integers. This is easily done, and the work is omitted here.

Lucas (l. c., p. 199) makes the statement that neither D_n nor S_n can be prime unless n is prime. The treatment in this section makes it easy to construct examples to show that this statement is not accurate. Thus if $\alpha + \beta = 1$ and $\alpha\beta = 2$, we have

$$D_4 = -3, \quad D_6 = 5, \quad D_8 = -3, \quad D_9 = -17, \quad D_{10} = -11,$$
$$D_{15} = -89, \quad D_{26} = 181; \quad S_9 = -5.$$

Equations (5) and (11) make it evident, however, that a prime value for D_n or S_n, when n is not prime, is of relatively rare occurrence.

5. Characteristic Factors of F_n, D_n, S_n.

The number $F_1 = \alpha - \beta$ is not in general an integer, but F_1^2 is always an integer. Consider then the sequence of integers $F_1^2, F_2, F_3, \cdots$. By a characteristic factor of F_n we mean a prime divisor of F_n which is not a factor of any number of the set $F_1^2, F_2, \cdots, F_{n-1}$.

Similarly, a characteristic factor of $D_n(S_n)$ is a prime divisor of $D_n(S_n)$ which is not a factor of any $D_\nu(S_\nu)$ for which ν is less than n.

Examples given in the preceding section show that when α and β are complex quantities it may often happen that F_n, D_n and S_n do not possess characteristic factors. Hence in the "existence theorems" of the present section we confine attention to the case when α and β are real.

From Theorem XIV we have the following result:

THEOREM XX. *A necessary and sufficient condition that a prime p which divides F_n shall be a characteristic factor of F_n is that p shall not be a divisor of n.*

From Theorems XVIII and XX it is easy to deduce the following:

THEOREM XXI. *If α and β are real and if $n \neq 1, 2, 6$, then $F_n(\alpha, \beta)$ contains at least one characteristic factor in all cases except when:* (*a*) *α and β are suitably chosen irrational numbers and n is equal to an odd prime divisor of* $(\alpha - \beta)^2$;

(*b*) $n = 3, \quad \alpha + \beta = \pm 1, \quad \alpha\beta = -2;$

(*c*) $n = 5, \quad \alpha + \beta = \pm 1, \quad \alpha\beta = -1;$

(*d*) $n = 12, \quad \alpha + \beta = \pm 1, \quad \alpha\beta = -1.$

From equations (5) and (11) follows the theorem:

THEOREM XXII. *A characteristic factor of $F_n(F_{2n})$ is also a characteristic factor of $D_n(S_n)$.*

Hence,*

THEOREM XXIII. *If α and β are real and $n \neq 1, 2, 6$, then D_n contains*

---

* Compare Birkhoff and Vandiver, l. c., p. 177, and Lucas, l. c., p. 291. For the case when α and β are integers Lucas states that for n sufficiently large it is "evident" that D_n has one or more characteristic factors. In what way the fact is "evident" is not clear.

at least one characteristic factor except when

$$n = 12, \quad \alpha + \beta = \pm 1, \quad \alpha\beta = -1.$$

THEOREM XXIV. *If* α *and* β *are real and* $n \neq 1, 3$, *then* S_n *contains at least one characteristic factor except when*

$$n = 6, \quad \alpha + \beta = \pm 1, \quad \alpha\beta = -1.$$

These results, together with Theorem XIX, lead to the following:

THEOREM XXV. *If* a *and* b *are relatively prime integers and* $n > 2$, *then* S_n *contains at least one characteristic factor except when*

$$n = 3, \quad a + b = \pm 3, \quad ab = 2,$$

while D_n *contains at least one characteristic factor except when*

$$n = 6, \quad a + b = \pm 3, \quad ab = 2.$$

Suppose now that p is an odd characteristic factor of $F_n(\alpha, \beta)$, $n > 1$. Then p is prime to $(\alpha - \beta)^2$ by definition of characteristic factor and to $\alpha\beta$ by Theorem I in connection with equation (5). Hence from Theorem XII it follows that p is a divisor of D_{p-1} or of D_{p+1} according as $(\alpha - \beta)^{p-1}$ is congruent to $+1$ or to -1 modulo p. From this, in view of equation (5) and Theorem XIV, it follows that n is a factor of $p - \left(\frac{\alpha, \beta}{p}\right)$, where $\left(\frac{\alpha, \beta}{p}\right) = +1$ or -1 according as $(\alpha - \beta)^{p-1}$ is congruent to $+1$ or to -1 modulo p. Hence p is of the form $p = kn + \left(\frac{\alpha, \beta}{p}\right)$, and we have the following theorem:

THEOREM XXVI. *A characteristic factor of* $F_n(\alpha, \beta)$ *is of the form* $kn + \left(\frac{\alpha, \beta}{p}\right)$.

COROLLARY. *If* a *and* b *are relatively prime integers a characteristic factor of* $F_n(a, b)$ *is of the form* $kn + 1$.

This theorem and corollary lead at once to the known results (Lucas, l. c., p. 291) concerning the form of the characteristic factors of D_n and S_n.

The above theorem gives the linear form of a characteristic factor of F_n. We may also determine a quadratic form of which F_n, and consequently any one of its factors, is a divisor. We have

$$(\alpha - \beta)^2 D_n^2 = S_n^2 - 4\alpha^n\beta^n,$$

as one may readily verify. Then, since F_n is a divisor of D_n by equation (5), if we take n odd we have at once the following result:

THEOREM XXVII. *The number* $F_{2k+1}(\alpha, \beta)$ *is a factor of the quadratic form* $x^2 - \alpha\beta y^2$.

The equation above may also be written

$$S_n^2 = 4\alpha^n\beta^n + (\alpha - \beta)^2 D_n^2 = \frac{4\alpha^{n+1}\beta^{n+1} + \alpha\beta(\alpha - \beta)^2 D_n^2}{\alpha\beta}.$$

Then, since F_{2n} is a divisor of S_n by equation (11) and is also prime to $\alpha\beta$ by Theorem I and equation (5), we have

THEOREM XXVIII. *The numbers* F_{4k+2} *and* F_{4k} *are divisors of the quadratic forms* $x^2 + \alpha\beta(\alpha - \beta)^2 y^2$ *and* $x^2 + (\alpha - \beta)^2 y^2$ *respectively.*

As an example let us consider the case when $\alpha\beta = 3$ and $\alpha + \beta$ is not divisible by 3. Then an odd characteristic factor of F_{2k+1} is a divisor of the quadratic form $x^2 - 3y^2$; and hence is of one of the linear forms $12z \pm 1$. It is also of one of the linear forms $m(2k + 1) \pm 1$. In particular a characteristic factor of F_{25} is of one of the forms

$$300s \pm 1, \qquad 300s \pm 49.$$

Moreover, F_{25} can contain no prime factor which is not characteristic unless $(\alpha - \beta)^2$ is a multiple of 5. But

$$(\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta,$$

and is not a multiple of 5, since this would require the impossible relation

$$(\alpha + \beta)^2 \equiv 2 \bmod 5.$$

Hence, in the present case, every prime factor of F_{25} is of one of the forms given above. As a particular example, if $\alpha + \beta = 2$, we have $F_{25} = 56{,}149$. Since this number is less than 299^2 and is not divisible by 251, it is easy to see that it must be prime.

6. Some Applications of the Preceding Results.

One of the results in Theorem XIV may be used to obtain a very simple proof of the following special case of Dirichlet's celebrated theorem concerning the prime terms of an arithmetical progression of integers:

THEOREM XXIX. *In the sequence of positive integers* $p^k x - 1$, *where* k *is a positive integer,* p *an odd prime and* x *runs over the set* $x = 1, 2, 3, \cdots$, *there is an infinitude of prime numbers.*

To prove this theorem we choose α and β so that $(\alpha - \beta)^2$ is a quadratic non-residue of p; that is, so that

$$(\alpha - \beta)^{p-1} \equiv -1 \bmod p.$$

That this is always possible is readily seen as follows: Let ρ be any quadratic non-residue of p of the form $4m + 1$. Let σ be any odd integer which is prime to ρ. Then write

$$(\alpha - \beta)^2 = \rho, \qquad \alpha + \beta = \sigma,$$

whence

$$\alpha\beta = \tfrac{1}{4}(\sigma^2 - \rho).$$

Then obviously $\alpha + \beta$ and $\alpha\beta$ are relatively prime integers; and therefore the determination of α and β from the above equations suffices for our purpose.

Now from the latter part of Theorem XIV we see that with these values of α and β we have

$$F_{p^{2r+1}} \equiv -1 \bmod p,$$

where r is a positive integer. Hence every prime factor of $F_{p^{2r+1}}$ is a characteristic factor; and any such factor, as we have seen before, is of the form $mp^{2r+1} - 1$. Consider the set of numbers

$$F_{p^{2r+1}}, \qquad r = 1, 2, 3, \cdots.$$

When $2r + 1$ is greater than k the rth number of the set contains a prime factor of the form $p^kx - 1$. But the numbers of the set are prime each to each (Theorem XV). Therefore there is an infinitude of primes of the form $p^kx - 1$, as was to be proved.

In a similar way, and even more readily, it may be shown that the sequence $nx + 1$, $x = 1, 2, 3, \cdots$, always contains an infinitude of prime numbers. For this result compare Lucas, l. c., p. 291, and Birkhoff and Vandiver, l. c., p. 177.

A large number of other special cases of Dirichlet's celebrated theorem may be simply proved by modifications of the foregoing method. This remark will be sufficiently illustrated by a proof of the following theorem:

THEOREM XXX. *There is an infinitude of prime numbers of the form* $2^k \cdot 3x - 1$, *where* k *is any positive integer.*

To prove this take

$$\alpha + \beta = 5, \qquad \alpha\beta = 7,$$

whence

$$(\alpha - \beta)^2 = -3.$$

Then (Theorem XXVIII) every divisor of F_{2n}, $n > 1$, is a factor of the quadratic form $x^2 - 3y^2$. If it is an odd prime it is therefore of one of the linear forms $12z + 1$, $12z - 1$. If $n \overset{=}{>} k$, it is also of one of the forms $2^kz + 1$, $2^kz - 1$. Hence it is of one of the forms $2^k \cdot 3x + 1$, $2^k \cdot 3x - 1$.

Now we have

$$F_{2n} = \alpha^{2n-1} + \beta^{2n-1} = (\alpha^{2n-2} + \beta^{2n-2})^2 - 2\alpha^{2n-2}\beta^{2n-2} = F_{2n-1} - 2\alpha^{2n-2}\beta^{2n-2};$$

and therefore in the present case F_{2^n} may be determined by the following method of recursion:

$$F_2 = 5, \quad F_{2^2} = 5^2 - 2 \cdot 7 = 11, \quad F_{2^3} = 11^2 - 2 \cdot 7^2 = 23, \quad \cdots.$$

It is obvious from this that every F_{2^n} is of the form $6k - 1$. Therefore, since every prime factor of F_{2^n}, $n \gtreqless k$, is of one of the forms $2^k \cdot 3x \pm 1$ it follows that for every n greater than k F_{2^n} contains at least one prime factor of the form $2^k \cdot 3x - 1$. Moreover F_{2^m} and F_{2^n} have no common factor (other than unity) when m and n are different (Theorem XV). Hence the set F_2, F_{2^2}, F_{2^3}, $\cdots$ contains as divisors an infinitude of prime numbers of the form $2^k \cdot 3x - 1$. Hence the theorem as stated above.

This theorem taken in connection with the fact that there is an infinitude of primes of the form $nx + 1$ leads to the following interesting corollary, also a special case of Dirichlet's theorem:

COROLLARY. *There is an infinitude of prime numbers of each of the forms* $4n + 1$, $4n - 1$, $6n + 1$, $6n - 1$.

7. On the Verification of Large Prime Numbers.

Lucas (l. c., pp. 301–317) has given some remarkable theorems which suffice for the determination of large prime numbers of given forms; these theorems grow out of a fundamental result which Lucas states essentially in the following form:

If D_ν *is divisible by* p *for* $\nu = p - 1$ *and for no value of* ν *which is a factor of* $p - 1$ *then* p *is prime; likewise, if* D_ν *is divisible by* p *for* $\nu = p + 1$ *and for no value of* ν *which is a divisor of* $p + 1$ *then* p *is prime.*

As thus stated the theorem is not entirely accurate; it fails when $p = 4$, as is shown by the following example:

$$\alpha + \beta = 3, \quad \alpha\beta = 1, \quad D_1 = 1, \quad D_2 = 3, \quad D_3 = 8.$$

The theorem is true, however, if the further restriction is made that p is odd. It becomes, then, a corollary of our Theorems XXXI and XXXVI below.

Some of our results concerning the numbers $F_n(\alpha, \beta)$ enable us to state general theorems which are related to those of Lucas, but are simpler in form and at the same time more far-reaching and complete. In this section we prove these theorems and develop certain of their consequences.

We begin with the following three closely related theorems:

THEOREM XXXI. *A necessary and sufficient condition that a given odd number* p *is prime is that there exist relatively prime integers* $\alpha + \beta$ *and* $\alpha\beta$ *such that* $F_{p-1}(\alpha, \beta)$ *is divisible by* p.

THEOREM XXXII. *A necessary and sufficient condition that a given odd number p is prime is that there exist relatively prime integers a and b such that* $F_{p-1}(a, b)$ *is divisible by p.*

THEOREM XXXIII. *A necessary and sufficient condition that a given odd number p is prime is that an integer a exists such that* $F_{p-1}(a, 1)$ *is divisible by p.*

For the demonstration of these *three* theorems it is obviously sufficient to prove the following two statements: If p is prime an integer a exists such that $F_{p-1}(a, 1)$ is divisible by p; if $F_{p-1}(\alpha, \beta)$ is divisible by p then p is prime. We consider separately the proofs of the two statements.

If p is an odd prime number then there exists a positive integer a (less than p) such that $a^x - 1$ is divisible by p for $x = p - 1$ but for no smaller value of x, as is well known from the theory of primitive roots modulo p. Hence $D_x(a, 1)$ is divisible by p for $x = p - 1$ but for no smaller value of x, since obviously $a - 1$ is prime to p. But

$$D_{p-1}(a, 1) = \Pi F_d(a, 1),$$

where d ranges over all the divisors of $p - 1$ except unity. Now, $F_d(a, 1)$, $d < p - 1$, is not divisible by p; for, if so, $D_d(a, 1)$ would be divisible by p. But the first member of the above equation contains p as a factor and hence the second does also; and therefore $F_{p-1}(a, 1)$ is a multiple of p. That is, when p is prime an integer a exists such that $F_{p-1}(a, 1)$ is divisible by p.

Now let us suppose that $F_{p-1}(\alpha, \beta)$ is divisible by p. From Theorem XIV it follows that $F_\nu(\alpha, \beta)$ is divisible by p only when ν is of the form $\nu = (p - 1)p^k$. Hence $D_\nu(\alpha, \beta)$ is divisible by p only when ν is a multiple of $p - 1$, as is readily seen from equation (5). But (Theorem XIII) if $\lambda = \lambda_{\alpha\beta}(p)$, $D_\lambda(\alpha, \beta)$ is divisible by p. Hence $\lambda_{\alpha\beta}(p)$ is a multiple of $p - 1$. Since p is odd it follows at once from this and the definition of $\lambda_{\alpha\beta}(p)$ that p is prime. Therefore, if $F_{p-1}(\alpha, \beta)$ is divisible by the odd number p then p is prime. This completes the demonstration of the theorems above.

Owing to the difficulty of reckoning out the value of F_{p-1} in general the above theorems are not convenient in practice for the verification that a given number p is prime unless p is of special form. Like all other known tests for determining the character of a number as to being prime they are usually unwieldy for purposes of reckoning. But that in particular cases of interest they give tests which are remarkably easy of application is evidenced by the special results which we are now to deduce.

Let p be of the form

$$p = 2^{2^n} + 1, \qquad n > 1.$$

Then

$$F_{p-1}(\alpha, \beta) = \alpha^{\frac{p-1}{2}} + \beta^{\frac{p-1}{2}},$$

as one may readily show.

Let r be any odd prime of which p is a quadratic non-residue. Then, if p is prime, r is likewise a quadratic non-residue of p, as the theorem of quadratic reciprocity shows. Hence when p is prime we have

$$r^{\frac{p-1}{2}} + 1 \equiv 0 \bmod p.$$

Furthermore, from Theorem XXXIII and the value of F_{p-1} in the present case, it follows that p is prime when the above congruence is satisfied. Hence we have the following theorem:*

THEOREM XXXIV. *If $p = 2^{2^n} + 1$, $n > 1$, and r is any odd prime of which p is a quadratic non-residue, then a necessary and sufficient condition that p is prime is that*

$$r^{\frac{p-1}{2}} + 1 \equiv 0 \bmod p.$$

COROLLARY. *A necessary and sufficient condition that $p = 2^{2^n} + 1$, $n > 1$, is prime is that*

$$3^{\frac{p-1}{2}} + 1 \equiv 0 \bmod p.$$

Thus it may be verified readily that

$$3^{2^{15}} + 1 \equiv 0 \bmod 2^{16} + 1,$$

whence it follows that $2^{16} + 1$, $= 65,537$, is a prime number.

In testing a given number p of the form $2^{2^n} + 1$ as to its prime character one would reckon out successively the residues modulo p of the numbers

$$3^2,\ 3^{2^2},\ 3^{2^3},\ 3^{2^4},\ \cdots.$$

If the νth residue is -1 and if this is the first one which is -1, then p is prime if and only if $\nu = n$. Furthermore, from Theorem XXVI, corollary, it follows that when ν is not equal to n the divisors of the composite number p are of the form $2^\nu k + 1$.

As another special case let us assume p to be of the form

$$p = 2^{k+1} \cdot q + 1,$$

---

* This theorem and corollary should be compared with a related theorem due to Pepin (see Comptes rendus de l'académie des sciences, Paris, 85 (1877): 329–331).

where q is an odd prime. Then from equation (10) we have

$$F_{p-1} = \frac{\alpha^{2^kq} + \beta^{2^kq}}{\alpha^{2^k} + \beta^{2^k}}.$$

Hence from XXXIII we have the following theorem:

THEOREM XXXV. *If* $p = 2^{k+1} \cdot q + 1$, *where* q *is an odd prime, then a necessary and sufficient condition that* p *is prime is that an integer* a *exists such that*

$$\frac{a^{2^kq} + 1}{a^{2^k} + 1} \equiv 0 \bmod p.$$

COROLLARY. *A necessary and sufficient condition that* $2^{k+1}3 + 1$ *is prime is that an integer* a *exists such that*

$$a^{2^{k+1}} - a^{2^k} + 1 \equiv 0 \bmod 2^{k+1}3 + 1.$$

It is obvious that such special theorems as these may be obtained in unlimited number from our general results in XXXI to XXXIII. It is unnecessary to develop them further. It is, however, desirable to say a word in regard to the matter of actual verification of large primes by means of these theorems. For this purpose it will be convenient to speak briefly concerning the corollary above. Having selected a number a for trial one would reckon out successively the residues of

$$a,\ a^2,\ a^{2^2},\ \cdots,$$

say

$$\rho_0,\ \rho_1,\ \rho_2,\ \cdots,$$

where

$$\rho_i^2 \equiv \rho_{i+1} \bmod 2^{k+1} \cdot 3 + 1.$$

Each number ρ_i is thus readily obtained from the preceding one. Now if

$$\rho_{k+1} - \rho_k + 1 \equiv 0 \bmod 2^{k+1} \cdot 3 + 1,$$

then $2^{k+1} \cdot 3 + 1$ is prime. It is thus seen that when the reckoning is carried out in an appropriate manner it can be done with rapidity.

Thus in order to verify that $2^{41} \cdot 3 + 1$ is prime it would be sufficient to reckon out successively 41 residues modulo p, each one being determined from the preceding one by squaring and reducing modulo p,—if we suppose that an appropriate choice of a has been made. But it is only in special cases that we may be certain, in advance of the reckoning, that an appropriate choice of a has been made. Compare the corollary to Theorem XXXIV.

As a correlative of Theorems XXXI to XXXIII we have the following:

THEOREM XXXVI. *A sufficient condition that an odd number p is prime is that there exist relatively prime integers $\alpha + \beta$ and $\alpha\beta$ such that*

$$F_{p+1}(\alpha, \beta) \equiv 0 \bmod p.$$

The proof is analogous to that employed in the demonstration of a part of Theorem XXXI. When $F_{p+1}(\alpha, \beta)$ is divisible by p it follows from Theorem XIV that $F_\nu(\alpha, \beta)$ is divisible by p when and only when ν is of the form

$$\nu = (p + 1)p^k.$$

Hence $D_\nu(\alpha, \beta)$ is divisible by p only when ν is a multiple of $p + 1$, as is readily seen from equation (5). But $D_\lambda(\alpha, \beta)$,

$$\lambda = \lambda_{\alpha\beta}(p),$$

is divisible by p, according to Theorem XIII; and therefore $\lambda_{\alpha\beta}(p)$ is a multiple of $p + 1$. It is obvious that this statement is true of an odd number p only when p is prime. Hence the theorem.

We shall now apply this general result to the determination of a necessary and sufficient condition that numbers of the form $2^n - 1$ shall be prime, thus obtaining as a corollary of our general theorem an important result which is due to Pepin (Comptes rendus de l'académie des sciences, Paris, 86 (1877): 307–310).

Suppose that $p = 2^n - 1$ is a prime number. Let r be a prime number of the form $4k + 1$ and write $r = a^2 + b^2$, where a and b are integers. Take

$$\alpha + \beta = 2a, \qquad \alpha\beta = a^2 + b^2,$$

whence

$$\alpha = a + b\sqrt{-1}, \qquad \beta = a - b\sqrt{-1}.$$

Suppose further that r is chosen so that p is a quadratic non-residue of r; then r is likewise a quadratic non-residue of p, as the law of quadratic reciprocity shows. Now Pepin (l. c., p. 307) has shown that if r is a quadratic non-residue of p, then

$$\alpha^{\frac{p+1}{2}} + \beta^{\frac{p+1}{2}} \equiv 0 \bmod p.$$

Applying this to the present case, we see that if p is prime it satisfies the relation

$$F_{p+1}(\alpha, \beta) \equiv 0 \bmod p.$$

But, according to the above theorem, if p satisfies this congruence it is prime. Hence we have the following corollary:

COROLLARY. *Let r be a prime number of the form $4k + 1$ of which $2^n - 1$ is a quadratic non-residue, and write $r = a^2 + b^2$ where a and b are integers. Put*

$$\alpha = a + b\sqrt{-1}, \qquad \beta = a - b\sqrt{-1}.$$

Then a necessary and sufficient condition that $2^n - 1$ is prime is that

$$F_{2^n} = \alpha^{2^{n-1}} + \beta^{2^{n-1}} \equiv 0 \bmod 2^n - 1.$$

It should be noticed, for purposes of reckoning, that we have the recurrence relation

$$F_{2^{k+1}} = F_{2^k}^2 - 2(\alpha\beta)^{2^k}$$

and that each of the terms of this equation represents an integer.

INDIANA UNIVERSITY,
November, 1912.